



IFW

PATENT  
B422-244 (25813.251)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s) : Masami Kugai  
Serial No. : 10/699,990  
Filed : November 3, 2003  
For : CONTENT UTILIZING METHOD  
Examiner : Kim Y. Vu  
Art Unit : 2135

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

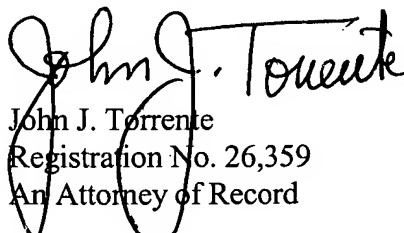
CLAIM TO BENEFIT OF 35 U.S.C. § 119  
AND FILING OF PRIORITY DOCUMENT

Claim is made herein to the benefit of 35 U.S.C. § 119 of the filing date of the following Japanese Patent Application: 2002-324169 (filed November 7, 2002) a certified copy of which is filed herewith.

Dated: September 22, 2004

Respectfully submitted,

COWAN, LIEBOWITZ & LATMAN, P.C.  
1133 Avenue of the Americas  
New York, NY 10036-6799  
(212) 790-92000

  
John J. Torrente  
Registration No. 26,359  
An Attorney of Record

BEST AVAILABLE COPY

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日 2002年11月7日  
Date of Application:

出願番号 特願2002-324169  
Application Number:

[ST. 10/C]: [JP 2002-324169]

願人 キヤノン株式会社  
Applicant(s):

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2003年11月25日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



出証番号 出証特2003-3096979

【書類名】 特許願

【整理番号】 223921

【提出日】 平成14年11月 7日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00  
G06F 17/00

【発明の名称】 コンテンツ配信システム

【請求項の数】 6

【発明者】

【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会社  
社内

【氏名】 久貝 正己

【特許出願人】

【識別番号】 000001007

【氏名又は名称】 キヤノン株式会社

【代理人】

【識別番号】 100090273

【弁理士】

【氏名又は名称】 國分 孝悦

【電話番号】 03-3590-8901

【手数料の表示】

【予納台帳番号】 035493

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705348

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ配信システム

【特許請求の範囲】

【請求項 1】 コンテンツの利用条件を選択する利用条件選択手段と、  
該利用条件選択手段により選択された利用条件を記憶する利用権スクリプトを  
生成する利用権スクリプト生成手段と、

あらかじめ用意されたか、またはユーザ情報に基づき作成される第 1 の暗号鍵  
によりコンテンツを暗号化するコンテンツ暗号化手段と、

該コンテンツ暗号化手段により暗号化されたコンテンツのデータと、コンテン  
ツ情報とを含むプログラムコードとしてのコンテンツパッケージを作成するコン  
テンツパッケージ作成手段と、

該コンテンツ情報、第 2 の暗号鍵、及び前記利用権スクリプトを含むライセン  
スコントロールを作成するライセンスコントロール作成手段と、

前記ライセンスコントロールを特定するためのライセンスコントロール情報含  
むユースチケットを生成するユースチケット生成手段と、

任意のデータを前記第 2 の暗号鍵で暗号化してできる認証データを生成する認  
証データ生成手段と、

該認証データ生成手段により生成される認証データを、前記第 2 の暗号鍵また  
はユーザが入力する第 3 の暗号鍵で正しく解読できるかどうかテストすることに  
より利用資格を認証する利用資格認証手段と、を備えたことを特徴とするコンテ  
ンツ配信システム。

【請求項 2】 ライセンスコントロールデータベースを備えたことを特徴と  
する請求項 1 に記載のコンテンツ配信システム。

【請求項 3】 前記利用権スクリプトは複数の利用権を記述でき、コンテン  
ツパッケージを実行するとその複数の利用権の中から利用権を選択して実行する  
ことを特徴とする請求項 1 に記載のコンテンツ配信システム。

【請求項 4】 利用権スクリプトには、利用権の実行に対する課金情報が記  
載され、利用権を実行するとライセンシーに課金処理がなされることを特徴とす  
る請求項 1 に記載のコンテンツ配信システム。

【請求項 5】 前記課金処理は、課金方式を選択させて行うようにしたことを特徴とする請求項 4 に記載のコンテンツ配信システム。

【請求項 6】 前記利用権の実行時に、課金チェックをすることを特徴とする請求項 4 または 5 に記載のコンテンツ配信システム。

#### 【発明の詳細な説明】

##### 【 0 0 0 1 】

##### 【発明の属する技術分野】

本発明は、コンテンツ配信システムに関し、特に、インターネットにおいてデジタルコンテンツを配信するに際し、著作権保護と、コンテンツの利用制御とを可能とするために用いて好適なものである。

##### 【 0 0 0 2 】

##### 【従来の技術】

近年、インターネットの普及によりデジタルコンテンツのネットワークを使つての配信による販売ビジネスが脚光を浴びている。しかしながら、一般にデジタルコンテンツの著作権を保護し対価を払わず利用されてしまう不正利用の恐れが問題となっている。

##### 【 0 0 0 3 】

そこで、ソニー社のMagicGateのように暗号・認証の技術を活用した著作権保護の技術があらわれている。しかし、このような技術は、メモリスティックのような暗号・認証機能を有した特殊な記録メディアを使用しなければならない。また、この方法は、デジタルコンテンツのコピー配信の便利さを活用できない方法となってしまう。

##### 【 0 0 0 4 】

また、従来のコンテンツ販売は、コンテンツそのものの対価を利用者から支払ってもらうやりかたであり、コンテンツを多く利用しても、少ししか利用しなくても利用者が支払う料金に違いがなく、利用者にとっては不都合な購入方法であった。

##### 【 0 0 0 5 】

##### 【発明が解決しようとする課題】

本発明は、上述の問題点に鑑みてなされたものであり、特別な記録メディアを必要とすることなく、著作権を保護しながらの自由なコンテンツ配信を可能にすることを第1の目的とする。

さらに、コンテンツの利用者の利用量に応じた対価の支払いを可能にすることを第2の目的とする。

#### 【0006】

##### 【課題を解決するための手段】

本発明は、上記課題を解決するために、コンテンツの利用条件を選択する利用条件選択手段と、該利用条件選択手段により選択された利用条件を記憶する利用権スクリプトを生成する利用権スクリプト生成手段と、あらかじめ用意されたか、またはユーザ情報に基づき作成される第1の暗号鍵によりコンテンツを暗号化するコンテンツ暗号化手段と、該コンテンツ暗号化手段により暗号化されたコンテンツのデータとコンテンツ情報を含むプログラムコードとしてのコンテンツパッケージを作成するコンテンツパッケージ作成手段と、該コンテンツ情報と第2の暗号鍵、及び前記利用権スクリプトを含むライセンスコントロールを作成するライセンスコントロール作成手段と、ライセンスコントロール情報を含むユースチケットを生成するユースチケット生成手段と、任意のデータを第2の暗号鍵で暗号化してできる認証データを生成する認証データ生成手段と、該認証データ生成手段により生成される認証データを第2の暗号鍵またはユーザが入力する第3の暗号鍵で正しく解読できるかどうかテストすることにより利用資格を認証する利用資格認証手段と、を備えたコンテンツ配信システム等を提供する。

#### 【0007】

##### 【発明の実施の形態】

本発明のコンテンツ配信システムの実施の形態の概要を説明する。

まず、コンテンツの購入を希望するユーザは、コンテンツのコマースサーバにアクセスして、気に入ったコンテンツが見付かったら、コンテンツのライセンスが提示する利用条件を利用条件選択手段により選択する。選択された利用条件は、利用権スクリプト生成手段により、利用権言語で表現された利用権スクリプトになる。

**【0008】**

コンテンツは第1の暗号鍵により暗号化され、コンテンツ情報を含むプログラム（例えばJava（R）アプレットの形式。以降これをコンテンツパッケージと呼ぶ）になる。該コンテンツ情報と第2の暗号鍵、及び前記利用権スクリプトを含むライセンスコントロールをライセンスコントロール作成手段により作成する。また、ユースチケット生成手段により、ライセンスコントロール情報及び第2の暗号鍵を含むユースチケットを生成する。なお、コンテンツのユーザが第3の暗号鍵（公開鍵暗号方式の秘密鍵）をあらかじめ有することを前提とするならば、ユースチケットは第2の暗号鍵を含まなくてよい。このライセンスコントロール情報は、前記作成されたライセンスコントロールを特定するための情報である。

**【0009】**

ユーザは、所定のPCまたはデジタル複合機に前記コンテンツパッケージとユースチケットをダウンロードする。以下、コンテンツパッケージがおかれているPCまたはデジタル複合機のことをコンテンツ実行機器と呼ぶ。

**【0010】**

また、コマー্সサーバからは、ライセンスコントロールが認証データ生成手段を備えた利用権コントロールサーバへ移されるか、コマー্সサーバが該認証データ生成手段を兼ね備えるならば、そのままコマー্সサーバにおかれる。以下、ライセンスコントロールの置かれたサーバを利用権コントロールサーバ（あるいは、UCS；Usage Control Serverと略す。）と呼ぶ。

**【0011】**

ユーザはコンテンツ実行機器でコンテンツパッケージを実行すると、コンテンツパッケージはユースチケットの中のライセンスコントロール情報を読み込み、利用権コントロールサーバに該ライセンスコントロール情報を転送する。利用権コントロールサーバでは、該ライセンスコントロール情報で対応するライセンスコントロールをUCSで管理されているライセンスコントロールデータベースの中から特定する。

**【0012】**

ライセンスコントロールに含まれるユーザ情報とコンテンツ情報と乱数を結合

したデータを第2の暗号鍵で暗号化して、認証データを作成する。利用権コントロールサーバは、この認証データをコンテンツ実行機器に送信し、コンテンツパッケージは、認証データをユースチケットに含まれる第2の暗号鍵またはユーザが入力する第3の暗号鍵で解読した復号データを利用権コントロールサーバへ送信する。利用権コントロールサーバはこの復号データを暗号化前のデータと一致するかどうかをチェックして認証に成功すれば、利用権スクリプトと第1の暗号鍵をコンテンツ実行機器へ送信する。コンテンツパッケージは、利用権スクリプトの利用条件にしがたいコンテンツを前記第1の暗号鍵で復号してから印刷や表示、演奏などを行う。

#### 【0013】

また、ライセンスコントロールが特定された以降の上述の利用資格認証処理の部分は次のようにしてもよい。UCSは、乱数を発生させて、乱数をコンテンツ実行機器に送信する。コンテンツ実行機器では、第2の暗号鍵またはユーザが入力する第3の暗号鍵で前記乱数を暗号化して認証データを作成する。この認証データをコンテンツパッケージがUCSに送信する。UCSがこの認証データをライセンスコントロールに含まれる第2の暗号鍵で復号し、復号されたデータが送信した乱数と一致するかどうかをチェックし認証を行う。

#### 【0014】

(第1の実施の形態)

次に、図面を参照しながら、本発明のコンテンツ配信システムの第1の実施の形態を以下に説明する。

#### 【0015】

図1は、本発明の実施の形態を示し、コンテンツ配信システムのシステム全体の構成を示したブロック図である。

1は、インターネットのネットワークである。2は、ユーザが使用するクライアントPC(端末)であり、インターネット1にHTTP、FTP、POP3、SMTPなどのプロトコルで接続されている。

#### 【0016】

3は、販売用コンテンツが置かれているコンテンツコマースサーバであり、や



はりインターネット 1 に接続されている。4 は、PC やネットワーク対応デジタル複写機のようなデバイスである。以降、デバイス 4 のことをコンテンツ実行機器と呼ぶことにする。

#### 【0017】

コンテンツ実行機器 4 は、インターネット 1 に接続するのに必要なソフトウェア (OS, インターネットの各種プロトコル、SSL、WWW ブラウザなど) と、Java (R) VM の環境を有している。

#### 【0018】

5 は、利用権コントロールサーバである。コンテンツ実行機器 4 と利用権コントロールサーバ 5 もインターネット 1 に接続されている。なお、コンテンツ実行機器 4 と利用権コントロールサーバ 5 は、同じ機能を一つに合体した 1 つのサーバであってもよい。

#### 【0019】

11、12、13 は、それぞれ後に説明するコンテンツパッケージ、ユースチケット、およびライセンスコントロールであって、システム内で扱われるデータを示している。

#### 【0020】

次に、図 2 のシステムフローに従って、本実施の形態のコンテンツ配信システムにおける処理を説明していく。図 2 は、ユーザがコンテンツを購入してから、利用料金を課金するまでの処理を示している。

#### 【0021】

まず、ユーザは自分の端末 2 からネットスケープナビゲータなどの Web ブラウザを使ってコンテンツコマースサーバ 3 にアクセスし、購入したいコンテンツが見付かったらコンテンツの購入指示を行う。そうすると、ステップ S201 において、コンテンツコマースサーバ 3 は、そのコンテンツの取引メニューをユーザの端末 2 のディスプレイの Web ブラウザに表示する。

#### 【0022】

図 3 は、コンテンツ取引メニューの画面を示している。取引メニュー画面 300 には、コンテンツ ID (301)、コンテンツ名 (302) と、選択できる利

用権とその課金方法が表示されている。図 3 の場合は、利用権が「印刷」権（3 0 3）しか表示されていないが、その他、「表示」権、「コピー」権などが表示される場合もある。

#### 【 0 0 2 3 】

また、図 3 では、印刷のオプションとして、白黒印刷かカラー印刷かを選択できるようにになっている。白黒かカラーかどちらを選択したかによって、対応した料金の金額が、金額表示欄 3 0 9、3 1 0、3 1 1、3 1 2 に表示されるようになってい

#### 【 0 0 2 4 】

3 0 3、3 0 4、3 0 5、3 0 6、3 0 7 は、チェックボックスであって、その項目が選択されると、チェックボックス 3 0 3、3 0 4、3 0 5、3 0 6、3 0 7 の中にチェックマーク（レ）が表示される。

#### 【 0 0 2 5 】

ユーザは、「印刷」3 0 3 を選択すると、次にオプションの「白黒」か「カラー」かのいずれかを選択する（ステップ S 2 0 2）。ここでは「カラー」が選択されたものとする。

そして、次に、課金方式を、実績課金方式 3 0 4 か、プリペイド方式 3 0 5 かのどちらにするかを選択する。

#### 【 0 0 2 6 】

実績課金方式 3 0 4 を選択すると、印刷の基本料金（コンテンツを利用しても利用しなくてもかかる料金）が 300 円であり、1 回の印刷につき、1200 円が課金されることになる。また、プリペイド方式 3 0 5 を選択すれば、ユーザがさらに、印刷回数が 2 回分のプリペイドをするか（チェックボックス（A）3 0 6）、1 0 回分のプリペイドをするか（チェックボックス（B）3 0 7）を選択する。

#### 【 0 0 2 7 】

チェックボックス（A）3 0 6 を選択すれば、2 回までの印刷ならば料金が 20 00 円、チェックボックス（B）3 0 7 を選択すれば 1 0 回までの印刷ならば 9000 円の料金となる。

#### 【 0 0 2 8 】

そして、308の「その他」はボタンとなっていて、これをマウスでクリックすると、チェックボックス（A）306、及びチェックボックス（B）307以外の印刷回数分をプリペイドする場合のプリペイド料金選択の画面へと移り（不図示）、ユーザは別の選択もできることになる。

#### 【0029】

ステップ203では、このようにしてユーザが課金方式を選択する。また、ユーザ固有のパスワード（以降ユーザキーと呼ぶ）をパスワード入力欄313に入力する。

#### 【0030】

314は、OKボタンであって、OKボタンを押すと取引メニュー画面300で入力した情報がコンテンツコマースサーバ3に送られる。なお、端末2とコンテンツコマースサーバ3との通信はSSLなどのプロトコルでセキュアな通信が確保されている。

#### 【0031】

315はキャンセルボタンで、これを押すと入力情報がクリアされ、再入力状態となる。

コンテンツコマースサーバ3は、取引メニュー画面300でユーザが指定した情報を受け取ると、つぎの3つを行う（ステップS204）。

#### 【0032】

第1に、コンテンツのデータを暗号化してコンテンツパッケージを生成する。

第2に、Usage Right Scriptを含むライセンスコントロールを生成する。

第3に、ユースチケットを生成する。

#### 【0033】

コンテンツのデータを暗号化するには、暗号鍵（コンテンツキーと呼ぶ）により例えばDESなどの共通鍵暗号方式で暗号化する。コンテンツキーは、あらかじめ定めた所定のものを使うか、もしくはコンテンツごと、取引ごと、ユーザごとにそれぞれ作成したものを使ってもよい。

#### 【0034】

また、コンテンツパッケージは、後述するプログラムコードのJava（R）アプ

レットである。コンテンツパッケージは、コンテンツIDやコンテンツ名などのコンテンツ情報も含む。

#### 【0035】

ユーザが取引メニューの画面 3 0 0 で必要事項を選択すると、選択した情報が、利用権スクリプト (Usage Right Script (以下、URSと略す)) というXML文法の言語で記述された利用権スクリプトを生成する。このURS 4 0 0 の例を図 4 に示す。また、図 5 は、URS 4 0 0 の文法の構造を示す。

#### 【0036】

図 5 の 5 0 1、5 1 0 ~ 5 1 3、5 2 0 ~ 5 2 2 は、すべてXMLのタグで挟まれたテキストデータである。例えば、コンテンツ情報 5 1 1 は、contentタグで囲まれ、<content>~</content>の形をしている。

#### 【0037】

ヘッダ部 5 1 0 は、スクリプト全体であり、このヘッダ部 5 1 0 の中に、コンテンツ情報 5 1 1、ライセンサ (コンテンツを使用許諾する者) 情報 5 1 2、ライセンシー (コンテンツの利用許諾を受ける者) 情報 5 1 3 が含まれている。

#### 【0038】

そして、5 2 0 は利用権の条件について記述される本体であって、この本体 5 2 0 の中に権利コード 5 2 1 の並びが含まれる。料金情報 5 2 2 には、権利コード 5 2 1 をユーザ (ライセンシー) が利用するときの課金情報が記述される。

#### 【0039】

URS 4 0 0 は、階層的な構造になっていて、下のブロックの記述内容は、上のブロックのタグに囲まれることを意味する。

権利コードには、Play, Print, Copy, Transfer, Loan, Delete がある。

Playは、コンテンツを表示・演奏・ゲームなどのプレイをする権利、Printは、コンテンツを印刷する権利、Copyは、コンテンツの複製を第3者に配信する権利、Transferは、コンテンツを第3者に譲渡する権利、Loanは、コンテンツを一時的に第3者に貸し出す権利、Deleteは、コンテンツを消去し払い戻しを受ける権利である。

#### 【0040】

図 4 の U R S のサンプル 4 0 0 において、4 0 1 はコンテンツ情報、4 0 2 はライセンス情報、4 0 3 はライセンシー情報、4 0 4 はPlay（表示）の権利コード、4 0 5 はPrintの権利コード、4 0 6 はCopyの権利コードの記述（コンテンツの権利をコピー配信する権利コードの記述）である。

Printの権利コード 4 0 5 の記述によると、印刷はカラーで印刷でき、2 回分の印刷の権利が2000円の料金で課金されることになっている。

#### 【 0 0 4 1 】

ライセンスコントロールには、取引メニュー画面 3 0 0 のパスワード入力欄 3 1 3 で入力したユーザキーと、U R S 4 0 0、コンテンツ情報、及びライセンスコントロール I D が含まれる。

#### 【 0 0 4 2 】

ここで、U R S 4 0 0 には、ユーザID、コンテンツIDが含まれるので、ユーザIDとコンテンツIDは、ライセンスコントロールに含まれることを注意しておく。ライセンスコントロールIDは、ライセンスコントロールに一意的につけられた I D 番号である。

#### 【 0 0 4 3 】

ステップ S 2 0 4 では、ユースチケットも生成される。ユースチケットには、ユーザキー、ライセンスコントロールIDが記憶されている。

#### 【 0 0 4 4 】

次に、ユーザは、ステップ S 2 0 5 で、必要なファイルをダウンロードする。コンテンツパッケージとユースチケットは、ユーザの管理下にあるインターネット 1 に接続されたコンテンツ実行機器 4 にダウンロードされる。

#### 【 0 0 4 5 】

また、ライセンスコントロール及びコンテンツキーは、コンテンツの売り手（ライセンス）の管理下にある利用権コントロールサーバ 5 に転送される。利用権コントロールサーバ 5 がコンテンツコマースサーバ 3 と同一のときは、ライセンスコントロールがコンテンツコマースサーバ 3 にそのまま置かれる。

#### 【 0 0 4 6 】

ステップ S 2 0 6 では、ユーザは自己の管理化にあるコンテンツ実行機器 4 で

コンテンツパッケージを実行する。コンテンツパッケージは、Java (R) アプレットであるので、Webブラウザから実行が可能である。

#### 【0 0 4 7】

コンテンツパッケージは、まず利用者がコンテンツを正規に購入したユーザであるかどうかの利用資格認証を行う。その利用資格の認証の具体的プロトコルを図6に示す。

#### 【0 0 4 8】

コンテンツパッケージは、利用権コントロールサーバ5とSSLのようなセキュアな通信セッションを確立する。そして、ユースチケットを読み込みライセンスコントロールIDを取得する。コンテンツパッケージは、ライセンスコントロールIDを利用権コントロールサーバ5へ送り、ユースチケットに対応するライセンスコントロールの検索を行うように要求をする(図6の①)。

#### 【0 0 4 9】

利用権コントロールサーバ(UCS)5は、多数のユーザが購入したライセンスについてのライセンスコントロールをデータベースとして管理している。

#### 【0 0 5 0】

利用権コントロールサーバ(UCS)5は、対応するライセンスコントロールを探し出し、乱数を発生させる。そして、ユーザIDとコンテンツIDとこの乱数を結合したデータを、ユーザキーで暗号化して認証データを作成する。本実施の形態では、このユーザキーを文字列であるパスワードとする。

#### 【0 0 5 1】

このように指定した文字列をキーとした暗号化は、例えば、UNIX(R)のCryptプログラムのような公知の技術を用いて行うようにすればよい。あるいは、ユーザキーを公開鍵暗号方式の公開鍵としてRSA、PGPのような暗号方式で暗号化すればよりセキュリティが高くなる。

#### 【0 0 5 2】

利用権コントロールサーバ(UCS)5は、認証データをコンテンツ実行機器4へ送り認証データの解読を要求する(図6の②)。コンテンツパッケージは、ユースチケットの中のユーザキーで認証データの解読をする。あるいは、認証デー

タの暗号化が公開鍵暗号方式を採用している場合は、ユーザの管理下にある秘密鍵データを使って解読をする。この場合は、秘密鍵を入力する操作が介入する。そして、解読した認証データを利用権コントロールサーバ（UCS） 5 に送信してチェックを要求する（図 6 の③）。

#### 【 0 0 5 3 】

利用権コントロールサーバ（UCS） 5 は、暗号化する前の認証データと、コンテンツ実行機器 4 から送られてきた解読された認証データとが等しいかどうかをチェックする。もし、等しくなければ、コンテンツ実行機器 4 のユーザは正規に利用資格を有していないと判断して、認証エラーをコンテンツ実行機器 4 へ送信して処理を終了する。もし、等しければコンテンツ実行機器 4 のユーザは利用資格を有していると判断して、ライセンスコントロール内の U R S 4 0 0 をコンテンツ実行機器 4 へ送信する（図 6 の④）。

#### 【 0 0 5 4 】

コンテンツ実行機器 4 では、送信されてきた U R S 4 0 0 が自分のものであるかどうかを、ユーザ情報を検査してチェックする。問題なければ、U R S 4 0 0 に基づき、利用メニューをコンテンツ実行機器 4 の表示機に表示する。

また、コンテンツをユースチケットのコンテンツキーで復号する（ステップ S 2 0 8）。

#### 【 0 0 5 5 】

例えば、図 4 の U R S 4 0 0 であると、Play(ディスプレイ)、Print、Copyの 3 つの権利が利用権メニューに表示される。

図 7 は、利用権メニューの一例である。図 7 の利用権メニュー画面 7 0 0 において、7 0 1 は、利用権を選択するためのチェックボックス、7 0 2 は、選択した利用権を実行する OK ボタン、7 0 3 は、処理を中止するキャンセルボタンである。

#### 【 0 0 5 6 】

ユーザは、この権利のうち実行したい権利を選ぶ（ステップ S 2 0 9）。例えば、Print（図 7 の印刷）を選んだとする。図 4 の例であると、Print は 2 回分のプリペイドの課金方式であるから、コンテンツパッケージは、支払いがなされて

いるか、すでに 2 回分の印刷を利用していないかなどをチェックする要求を利用権コントロールサーバ (UCS) 5 に出す (図 6 の⑤)。

#### 【0 0 5 7】

利用権コントロールサーバ (UCS) 5 は、これらをチェックし問題があれば課金チェックエラーをコンテンツ実行機器 4 に送信する (ステップ S 2 1 0)。課金チェックエラーを受信するとコンテンツパッケージは処理を終了する。課金チェックに問題なければ OK を送信する (図 6 の⑥)。

#### 【0 0 5 8】

コンテンツパッケージが OK を受信すると、Print の権利を実行する (ステップ S 2 1 1)。実行が正常におわれば、利用権コントロールサーバ (UCS) 5 に課金処理を依頼する (図 6 の⑦、図 2 のステップ S 2 1 2)。

#### 【0 0 5 9】

利用権コントロールサーバ (UCS) 5 では、当該ライセンスコントロールに記述されているライセンシーに対して相応の課金をすることになる。利用権コントロールサーバ (UCS) 5 にはライセンシーに対して売掛金を記憶する記憶領域 (売掛金口座) が用意されており、課金された金額がその売掛金口座に対して追加加算される。そして、例えば毎月末に口座残高をライセンシーに請求する。

#### 【0 0 6 0】

この場合は、プリペイド課金方式であるので、ライセンスコントロール (URS 4 0 0 を含む) を作成したとき (ステップ S 2 0 4) に売掛金に加算されていて、ステップ S 2 1 2 では前払いしている利用可能残数を減らす処理が行われる。

#### 【0 0 6 1】

また、実績課金方式が設定された権利が実行された場合は、ステップ S 2 1 2 で URS 4 0 0 に指定された条件の金額が、売掛金口座に加算される。

#### 【0 0 6 2】

以上のように本実施の形態では、端末 2 に表示される取引メニュー画面 3 0 0 の内容に従ってユーザが指定した情報をコンテンツコマースサーバ 3 が受け取ると、コンテンツパッケージとユースチケットをコンテンツ実行機器 4 にダウンロードするとともに、ライセンスコントロールを利用権コントロールサーバ 5 に転



送する。そして、利用権コントロールサーバ5は、転送されたライセンスコントロールの中のユーザキーを用いて、対応するライセンスコントロールを暗号化して認証データを作成し、コンテンツ実行機器4に送る。コンテンツ実行機器4は、ユースチケットの中のユーザキーを用いて、送られた認証データを解読し、利用権コントロールサーバ5に送信する。利用権コントロールサーバ5は、暗号化する前の認証データと解読された認証データとが等しければ、コンテンツ実行機器4のユーザは利用資格を有していると判断して、ライセンスコントロールの中の利用権スクリプト400とコンテンツキーをコンテンツ実行機器4へ送信する。コンテンツ実行機器4では、送信されてきた利用権スクリプト400が自分のものであるかどうかを、ユーザ情報を検査してチェックして問題なければ、利用権スクリプト400に基づき、利用メニューをコンテンツ実行機器4の表示機に表示するとともに、コンテンツをユースチケットのコンテンツキーで復号する。

#### 【0063】

以上のように構成することにより、コンテンツパッケージは暗号化されているので、コンテンツパッケージを配信しても、不正利用することはできない。

また、ユースチケットをユーザが他の第3者に与えてしまうと、第3者はそのユースチケットにかかれたユーザの支払いで不正利用する恐れはある。しかし、これはユーザの不利益になるので、通常ユーザはユースチケットを自己の個人情報として機密に管理するはずであるので大きな問題は生じない。

#### 【0064】

したがって、特別な記録メディアを用いなくてもコンテンツパッケージの自由な配信が可能であり、コンテンツの流通を拡大することができる。これは、特別な記録メディア（ハードウェア）の仕組みを使って著作権を保護する従来の技術では実現できなかったことである。

#### 【0065】

また、コンテンツの利用対価の支払いについても、コンテンツ利用者は利用度数に応じて支払うという課金方法の恩恵をうることができる。これは、コンテンツそのものの対価を利用者から支払ってもらう従来のやり方よりも大変都合のいいものである。

**【 0 0 6 6 】**

(第 2 の実施の形態)

次に、本発明の第 2 の実施の形態について説明する。なお、本実施の形態は、上記の第 1 の実施の形態と利用資格の認証方法が異なる。すなわち、本実施の形態のコンテンツ配信システムは、図 6 に示した利用資格の認証を図 8 に示す方法に置き換えたものである。したがって、ここでは利用資格の認証についてのみ説明し、その他の説明を省略する。

**【 0 0 6 7 】**

図 8 において、利用権コントロールサーバは、乱数を生成して乱数をコンテンツ実行機器へ送信する ( 8 0 1 ) 。コンテンツパッケージは、乱数を受信し、第 2 の暗号鍵または第 3 の暗号鍵 ( この第 3 の暗号鍵は公開鍵暗号方式におけるユーザの秘密鍵であり、この場合第 2 の暗号鍵は該秘密鍵に対応する公開鍵になる。 ) で乱数を暗号化して認証データを作り、これを利用権コントロールサーバ ( UCS ) へ送信する ( 8 0 2 ) 。利用権コントロールサーバ ( UCS ) は、受信した認証データをライセンスコントロールに含まれる第 2 の暗号鍵でこれを復号し、送信前の乱数と比較する。一致すれば、利用資格があるとして URS をコンテンツ実行機器に送る ( 8 0 3 ) 。一方、一致しなければ利用資格がないものとして、例えば認証エラーをコンテンツ実行機器 4 へ送信して処理を終了する。

**【 0 0 6 8 】**

このように本実施の形態では、利用権コントロールサーバ 5 とコンテンツ実行機器 4 との間で乱数を送受信することにより利用資格の認証を行うようにしたので、利用資格の認証を容易且つ確実に行うことができる。

**【 0 0 6 9 】**

(本発明の他の実施形態)

上述した実施形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、前記実施形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ ( CPU あるいは MPU ) に格納されたプログラムに従って前記各種デバイスを動作させることによって実施したもの

も、本発明の範疇に含まれる。

#### 【0070】

また、この場合、前記ソフトウェアのプログラムコード自体が上述した実施形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えば、かかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性のメモリカード、ROM等を用いることができる。

#### 【0071】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているOS（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施形態に含まれることは言うまでもない。

#### 【0072】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を行ない、その処理によって上述した実施形態の機能が実現される場合にも本発明に含まれることは言うまでもない。

#### 【0073】

##### 【発明の効果】

以上説明したように本発明によれば、コンテンツパッケージは暗号化されているので、コンテンツパッケージを配信しても、不正利用はできない。

したがって、コンテンツパッケージの自由な配信が可能であり、コンテンツの流通を拡大することができる。これは、特別なハードウェアの仕組みを使って著作権を保護する従来技術では実現できなかったことである。

#### 【0074】

また、コンテンツの利用対価の支払いについても、コンテンツの利用者は、コンテンツの利用度数に応じて支払うという課金方法の恩恵を受けることができる。これは、従来のやり方よりも大変都合のいいものである。

#### 【図面の簡単な説明】

##### 【図 1】

本発明の第 1 の実施の形態を示し、コンテンツ配信システムのシステム全体の構成を示したブロック図である。

##### 【図 2】

本発明の第 1 の実施の形態を示し、コンテンツ配信システムにおける処理を説明するフローチャートである。

##### 【図 3】

本発明の第 1 の実施の形態を示し、コンテンツ取引メニューの画面の一例を示した図である。

##### 【図 4】

本発明の第 1 の実施の形態を示し、利用権スクリプトの一例を示した図である。

##### 【図 5】

本発明の第 1 の実施の形態を示し、利用権スクリプトの構造の一例を示した図である。

##### 【図 6】

本発明の第 1 の実施の形態を示し、利用資格の認証のプロトコルを説明する図である。

##### 【図 7】

本発明の第 1 の実施の形態を示し、利用権メニューの一例を示した図である。

##### 【図 8】

本発明の第 2 の実施の形態を示し、利用資格の認証のプロトコルを説明する図である。

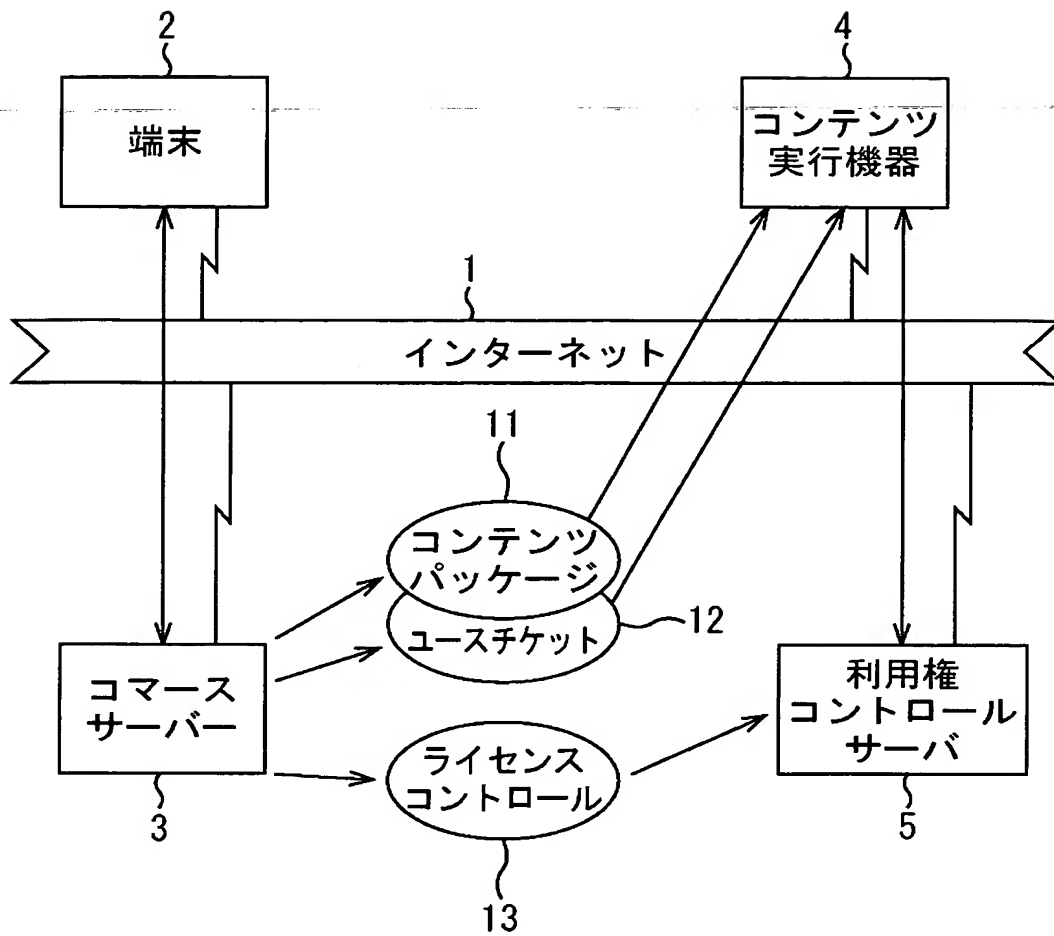
#### 【符号の説明】

1 インターネット

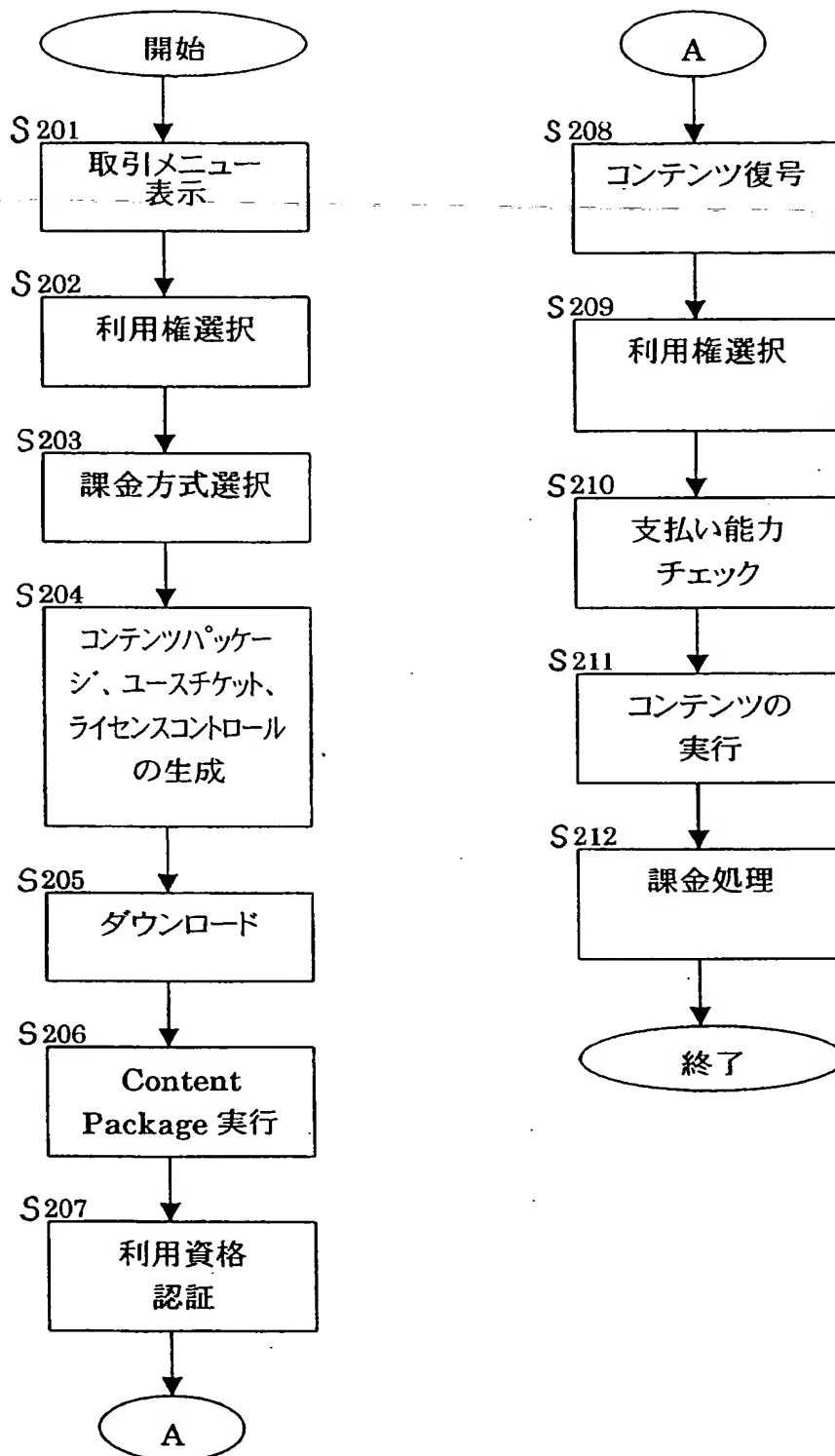
- 2 端末
- 3 コンテンツコマーサーバ
- 4 コンテンツ実行機器
- 5 利用権コントロールサーバ
- 1 1 コンテンツパッケージ
- 1 2 ユースチケット
- 1 3 ライセンスコントロール
- 3 0 0 取引メニュー画面
- 7 0 0 利用権メニュー画面

【書類名】 図面

【図 1】



【図 2】



【図 3】

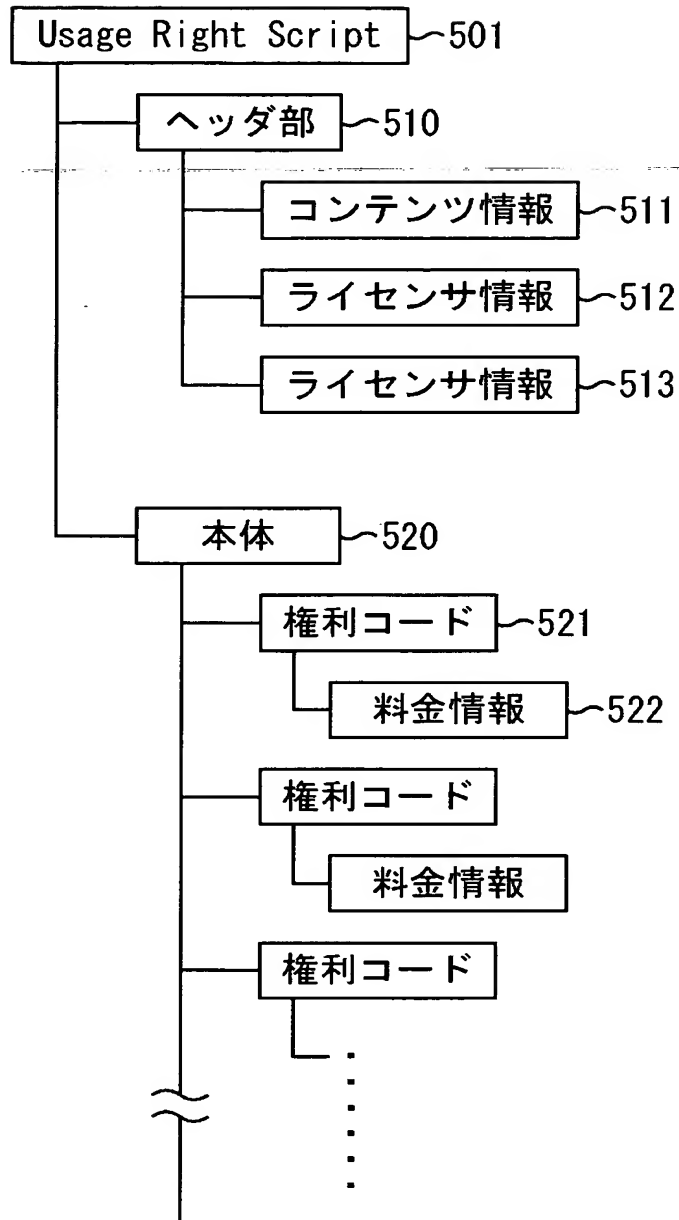
300

取引メニュー		
301	→	コンテンツ I D : gdoc023655
302	→	コンテンツ名 : 浦島太郎の昔話についての考察
利用権		
<hr/>		
303	→	<input type="checkbox"/> 印刷 <input type="radio"/> 白黒 <input checked="" type="radio"/> カラー
304	→	<input type="checkbox"/> <料金—実積課金方式—>
		基本料金 <input type="text" value="300"/> 円      309
		1回の印刷料金 <input type="text" value="1200"/> 円      310
305	→	<input type="checkbox"/> <料金—プリペイド方式—>
		回数      前払い料金      311
306	→	<input type="checkbox"/> A      2 <input type="text" value="2000"/> 円      312
307	→	<input type="checkbox"/> B      10 <input type="text" value="9000"/> 円
308	→	<input type="text" value="その他"/>
<hr/>		
パスワード		<input type="text"/> ← 313
<hr/>		
<div>OK      キャンセル</div>		
<div>↑      ↑</div>		
<div>314      315</div>		

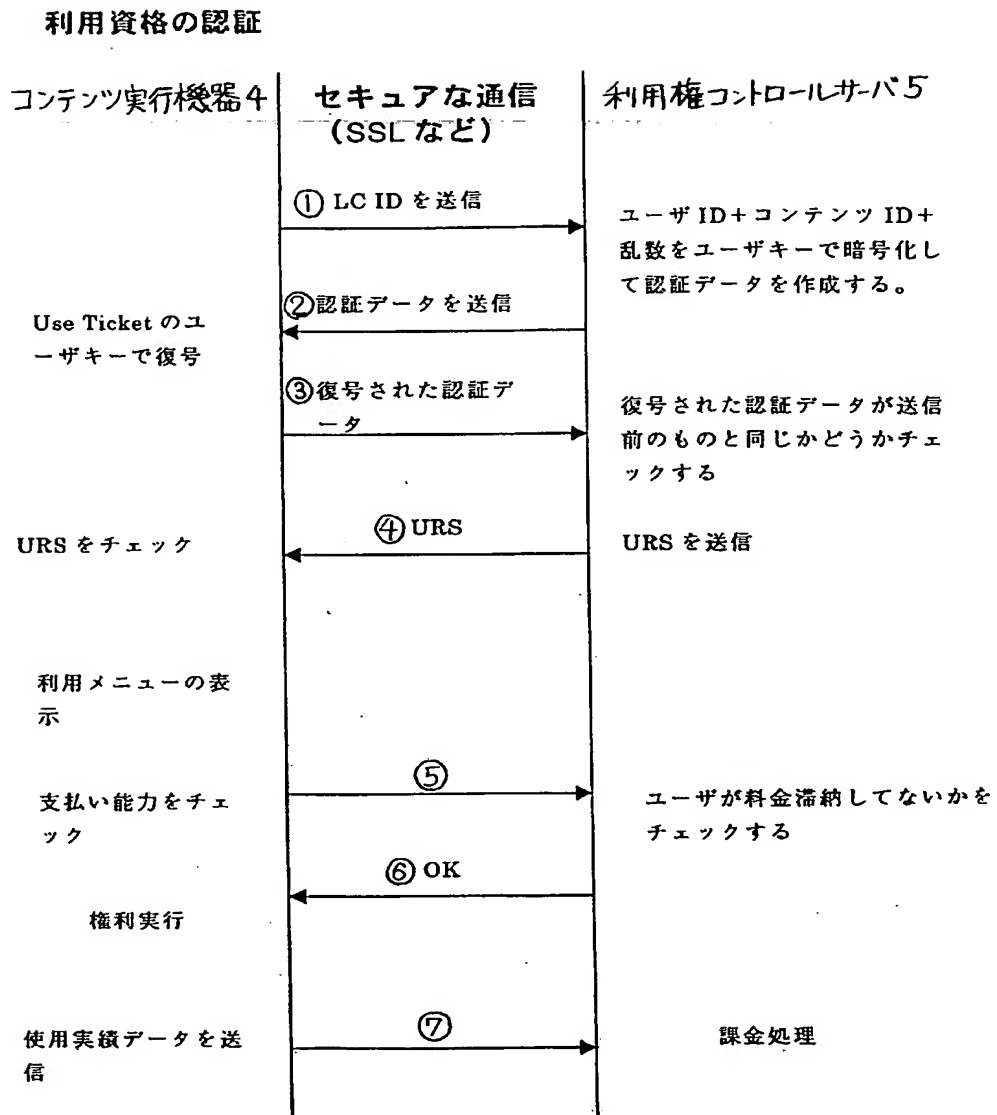




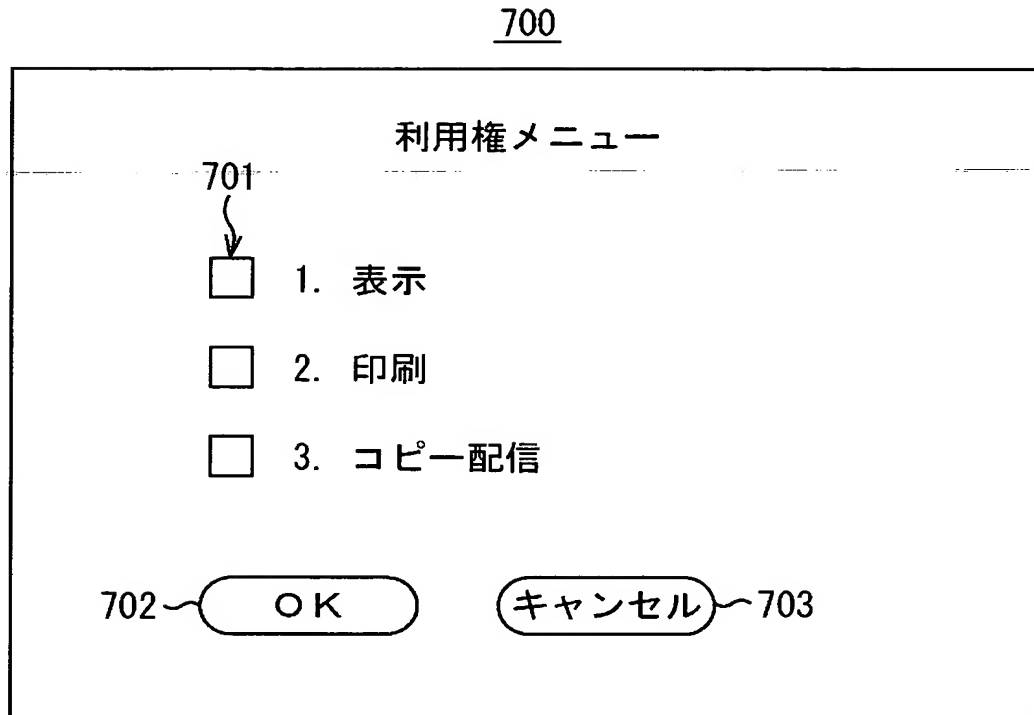
【図 5】



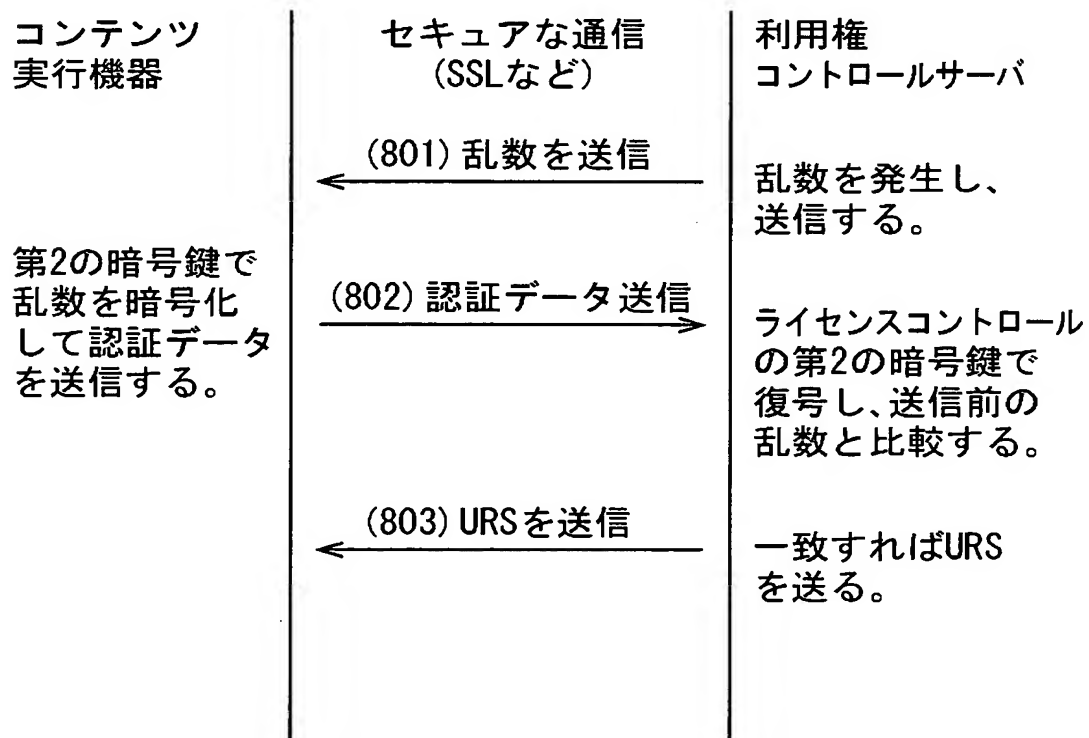
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 特別な記録メディアを必要とすることなく、著作権を保護しながらの自由なコンテンツ配信を可能にする。

【解決手段】 コンテンツの利用条件を選択し、選択した利用条件を記憶する利用権スクリプトを生成し、第 1 の暗号鍵によりコンテンツを暗号化し、暗号化したコンテンツのデータ及びコンテンツ情報を含むコンテンツパッケージと、上記コンテンツ情報、第 2 の暗号鍵、及び上記利用権スクリプトを含むライセンスコントロール情報と、上記ライセンスコントロール情報を含むユースチケットとを生成し、任意のデータを第 2 の暗号鍵で暗号化してできる認証データを生成し、生成した認証データを第 2 の暗号鍵またはユーザが入力する第 3 の暗号鍵を用いて正しく解読できるかどうかをテストして利用資格を認証するコンテンツ配信システムを提供する。

【選択図】 図 1

特願 2 0 0 2 - 3 2 4 1 6 9

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 1 0 0 7 ]

1. 変 更 年 月 日

1 9 9 0 年 8 月 3 0 日

[ 変 更 理 由 ]

新 規 登 録

住 所

東 京 都 大 田 区 下 丸 子 3 丁 目 3 0 番 2 号

氏 名

キヤノン株式会社